(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
7 février 2002 (07.02.2002)

PCT

(10) Numéro de publication internationale
WO 02/10918 A1

(51) Classification internationale des brevets[7] : G06F 9/46, G07F 7/10, H04Q 7/32

(21) Numéro de la demande internationale :
PCT/FR01/02489

(22) Date de dépôt international : 30 juillet 2001 (30.07.2001)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
00/10088 31 juillet 2000 (31.07.2000) FR

(71) Déposant *(pour tous les États désignés sauf US)* : ALCATEL [FR/FR]; 54, rue La Boétie, F-75008 Paris (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : DURAND, Romain [FR/FR]; 3, rue de Miromesnil, F-75008 Paris (FR). HELAINE, Hubert [FR/GB]; 206, Hurricane Way, Woodley Reading, Berkshire RG5 4UH (GB).

(74) Mandataires : LE FLOCH, Claire etc.; Compagnie Financière Alcatel, Département Propriété Industrielle, 30, avenue Kléber, F-75116 Paris (FR).

(81) États désignés *(national)* : AU, CN, JP, US.

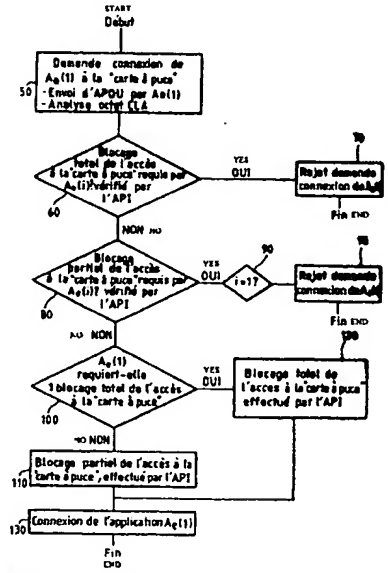
Déclaration en vertu de la règle 4.17 :
— *relative à la qualité d'inventeur (règle 4.17.iv)) pour US seulement*

Publiée :
— *avec rapport de recherche internationale*

[Suite sur la page suivante]

(54) Title: METHOD FOR MAKING SECURE ACCESS TO A RESIDENT APPLICATION ON A USER CARD CO-OPERATING WITH A COMMUNICATION SYSTEM TERMINAL, AND CORRESPONDING TERMINAL

(54) Titre : PROCEDE DE SECURISATION DE L'ACCES A UNE APPLICATION RESIDANTE SUR UNE CARTE UTILISATEUR COOPERANT AVEC UN TERMINAL D'UN SYSTEME DE COMMUNICATION, ET TERMINAL CORRESPONDANT



50 - REQUEST FROM A(1) TO THE SMART CARD SENDING APDU WITH Ae(1)... ANALYSING CLA OCTET
60 - TOTAL BLOCKING OF ACCESS TO THE SMART CARD BY Ae(1) VERIFIED BY THE API
70 DENY CONNECTION REQUEST FROM A(1)
80 - PARTIAL LOCKING OF ACCESS TO THE SMART CARD REQUESTED BY A(1) VERIFIED BY API
90 DENY CONNECTION REQUEST FROM A(1)
100 DOES A(1) REQUIRE TOTAL BLOCKING OF ACCESS TO THE SMART CARD ?
120 TOTAL BLOCKING OF ACCESS TO SMART CARD PRODUCED BY API
110 PARTIAL BLOCKING OF ACCESS TO SMART CARD PRODUCED BY API
130 CONNECTION OF APPLICATION A(1)

(57) **Abstract:** The invention concerns a method for making secure the access of an external application to at least a microprocessor user card, said user card being capable of containing several internal applications, said external application corresponding to one of the internal applications, said user card co-operating with a terminal, said external application using a connection protocol to the user card wherein, with each external application is associated a predetermined identification parameter. Said method comprises the following steps: when a first external application is connected to the corresponding internal application on said user card, determining the application identification parameter; if a second external application requires connection to said user card, analysing the parameter identification of said second application; if said parameter is identical to that of the first connected application, prohibiting access for the second external application to said corresponding internal application on the user card.

(57) **Abrégé :** Procédé pour sécuriser l'accès d'une application externe à au moins une carte utilisateur à microprocesseur, ladite carte utilisateur étant susceptible de contenir plusieurs applications internes, ladite application externe correspondant à une des applications internes, ladite carte utilisateur coopérant avec un terminal, ladite application externe utilisant un protocole de connexion à ladite carte utilisateur dans lequel, à chaque type d'application externe est associé un paramètre d'identification prédéterminé, comportant les étapes suivantes: lorsqu'une première application externe est en connexion avec l'application interne correspondante sur ladite carte utilisateur, on détermine le paramètre d'identification de l'application, si une deuxième application externe requiert la connexion à ladite carte utilisateur, on analyse le paramètre d'identification de ladite deuxième application, si ledit paramètre est identique à celui de la première application connectée, on interdit l'accès pour ladite deuxième application externe à ladite application interne correspondante sur la carte utilisateur.

WO 02/10918 A1

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

PROCEDE DE SECURISATION DE L'ACCESS A UNE APPLICATION RESEDANTE SUR UNE CARTE UTILISATEUR COOPERANT AVEC UNE TERMINAL D'UN SYSTEME DE COMMUNICATION, ET TERMINAL CORRESPONDANT

La présente invention concerne un procédé de sécurisation de l'accès à au moins une application supportée par une carte utilisateur à microprocesseur. Cette carte utilisateur coopère avec un des terminaux de communication d'un système de communication. L'invention concerne également un terminal de communication mettant en œuvre ce procédé.

Un des domaines d'application, non exclusif, de l'invention est celui des terminaux mobiles de radiocommunication fonctionnant dans un système de radiocommunication cellulaire. L'invention s'applique notamment, mais non exclusivement, à un système selon le standard GSM (Groupe spécial Systèmes Mobiles publics de radiocommunication).

Les terminaux d'un système de radiocommunication peuvent coopérer avec au moins une carte à puce intelligente, appelée en anglais "smart card". Chaque carte à puce contient au moins une application interne. Chaque application interne est susceptible de coopérer avec une application externe à la carte à puce. Par exemple, l'application externe peut être une application bancaire coopérant avec une carte utilisateur de type carte de paiement supportant l'application bancaire correspondante.

De plus, lorsqu'une application externe désire accéder à l'application interne correspondante supportée par la carte à puce, cette application externe commence le protocole de connexion. Elle échange des données dites APDU (Applicative Protocol Data Unit en anglais : Unité d'échange de données de niveau applicatif) via l'interface logicielle du terminal ou API (Application Programming interface en anglais : Interface de programmation de et vers l'application). Dans l'APDU, l'application externe indique son type (bancaire, ou autres) ou classe. Cette classe est indiquée dans l'un des octets de l'APDU, appelé octet "CLA".

Le concept de plusieurs applications réunies sur une même carte est très avantageux pour l'abonné. En effet, celui-ci peut effectuer de façon simple et uniquement avec son terminal de nombreuses opérations telles que le paiement d'une commande effectuée également depuis son terminal.

Ainsi, plusieurs applications externes différentes peuvent avoir accès simultanément aux applications internes correspondantes sur la même carte à puce. Mais deux applications externes identiques ne doivent pas avoir accès simultanément à l'application interne correspondante sur la "smart card".

Cette restriction d'accès doit être possible pour pallier les risques d'utilisation frauduleuse des applications de la carte à puce. Dans le cas d'une transaction entre une application externe bancaire et l'application bancaire de la carte à puce d'un abonné, une transaction entre une application pirate de type bancaire demandant l'accès à la "smart card" de l'abonné doit être évitée.

D'autre part, au sein d'une carte à puce contenant plusieurs applications internes différentes, l'étanchéité entre les différentes applications internes est difficilement garantie. Ainsi, prenons le cas d'une première application externe X est déjà en communication avec l' application interne X correspondante située sur la carte à puce. Si une application externe pirate X' veut communiquer avec l'application interne X, alors l'application X' pourrait se connecter sur une application interne Y située dans la carte à puce à proximité de l'application interne X. Puis cette application X' pourrait profiter d'un éventuel manque d'étanchéité entre les applications internes pour atteindre l'application interne X.

Dans l'état de la technique, on connaît le modèle du tout ou rien. Ce modèle fonctionne par exemple sur les équipements tel que les terminaux de communication permettant l'accès à internet ou "internet communication terminal" en anglais. Sur ce genre de terminaux, des applications peuvent être téléchargées de l'extérieur.

Si le protocole de connexion utilisé par l'application externe est connu par le terminal alors l'application externe est dite "application autorisée" et peut accéder à l'application interne correspondante de la carte à puce. Cependant, si une autre application externe autorisée, et ayant la même classe que la première, demande l'accès à la même application interne de la carte à puce, la deuxième application peut également accéder à la même application interne sur la carte à puce et une interférence entre les deux applications externes a lieu.

La solution antérieure n'est donc pas suffisante pour pallier le risque évoqué ci-dessus.

L'invention résout ce problème en permettant à une application externe de réserver l'accès à l'application interne correspondante de la carte utilisateur pour elle seule.

De manière plus précise, l'invention a pour objet un procédé pour sécuriser l'accès d'une application externe à au moins une carte utilisateur à microprocesseur.

Ladite carte utilisateur est susceptible de contenir plusieurs applications internes, ladite application externe correspondant à une des applications internes.

Ladite carte utilisateur coopère avec un terminal.

Ladite application externe utilise un protocole de connexion à ladite carte utilisateur dans lequel, à chaque type d'application externe est associé un paramètre d'identification prédéterminé. Ce procédé comporte les étapes suivantes :

- lorsqu'une première application externe est en connexion avec l'application interne correspondante sur ladite carte utilisateur, on détermine le paramètre d'identification de l'application,
- si une deuxième application externe requiert la connexion à ladite carte utilisateur, on analyse le paramètre d'identification de ladite deuxième application,
- si ledit paramètre d'identification est identique à celui de la première application connectée, on interdit l'accès pour ladite deuxième application externe à ladite application interne correspondante sur la carte utilisateur.

En particulier, le procédé comporte un protocole de connexion entre l'application externe et l'application interne correspondante sur la carte utilisateur. Ce protocole résulte d'un échange d'APDU, contenant plusieurs octets, entre l'application externe et l'application interne située sur la carte utilisateur via l'interface logicielle du terminal, ledit paramètre d'identification étant représenté par au moins l'un des octets de l'APDU.

Le procédé comporte un protocole de connexion pendant lequel a lieu un échange d'APDU tel qu'au moins l'un des octets de l'APDU est l'octet CLA définissant la classe de l'application externe, chaque type d'application externe identique, susceptible de pouvoir échanger des APDU ayant un octet CLA identique, ledit paramètre d'identification étant l'octet CLA.

Le procédé est tel que l'application externe d'une classe définie ayant effectué une réservation totale de l'accès à au moins une carte utilisateur, l'analyse dudit paramètre d'identification par l'interface logicielle sera effectuée sur toutes les classes possibles qui définissent une application externe.

D'autres caractéristiques et avantages de l'invention apparaîtront à la lecture de la description suivante se rapportant à un mode de réalisation donné à titre d'exemple mais en aucun cas limitatif. Ce mode de réalisation fait référence aux dessins annexés.

La figure 1 est un schéma synoptique d'une donnée de type APDU.

La figure 2 est un schéma synoptique simplifié du dispositif selon l'invention mettant en œuvre le procédé de sécurisation d'accès selon l'invention.

La figure 3 est un organigramme du procédé de sécurisation de l'accès selon l'invention.

En référence à la figure 1, lorsqu'une application externe désire accéder à l'application interne correspondante supportée par la carte à puce située dans un terminal d'un système de radiocommunication, cette application commence le protocole de connexion et échange des données dites APDU 1 avec le terminal. Cet APDU contient plusieurs octets. L'un de ces octets est l'octet CLA 2. Cet octet indique la classe de l'application externe. Deux applications externes de même type ont la même classe, par exemple deux applications de type bancaire.

En référence à la figure 2, chaque terminal d'un système de radiocommunication coopère avec au moins une carte à puce 40. Chaque carte à puce 40 peut contenir plusieurs applications internes correspondant 15, 25, 35 à des applications externes 10, 20, 30.

Chaque application externe Ae(i) d'un type donné possède une classe donnée telle que CLA[Ae(i)]=i.

Deux applications externes Ae(1) et Ae(2) 10 et 20 de type différent, donc de classe différente, auront un octet CLA de valeur différente CLA[Ae(1)]=1 et CLA[Ae(2)]=2.

Cette application externe peut être locale, telle l'application GSM d'un terminal GSM; ou peut être distante telle une application bancaire communiquant avec l'application bancaire de la "smart card".

Dans ce qui suit, on entend par "blocage total", ce blocage total de l'accès à l'API donc à la carte à puce ayant été requis par une application externe, l'interdiction de l'accès à la carte à puce pour n'importe quelle autre application externe quelque soit sa classe.

On entend également par "blocage partiel", ce blocage partiel de l'accès à l'API donc à la carte à puce ayant été requis par une première application externe, l'interdiction de l'accès à la carte à puce pour une deuxième application externe de même classe que la première.

Sur la figure 3, dans l'étape 50, une application externe Ae(1) demande l'accès à l'application interne Ai(1) contenue dans une carte à puce d'un terminal d'un système de radiocommunication. Cette application externe envoie des données de type APDU pendant le protocole de connexion via l'interface logicielle du terminal (API). A cette application externe est associé un paramètre d'identification prédéterminé : l'octet CLA contenu dans l'APDU et tel que CLA[Ae(1)]=1. On analyse la valeur de l'octet CLA.

Ensuite, dans l'étape 60, l'API vérifie si l'accès à la "smart card" est bloqué par une autre application externe Ae(i) qui aurait demandé le blocage de l'accès à la carte à puce pour une autre application quelle que soit sa classe (ce qui constitue le blocage total) :

Si c'est le cas, alors on passe à l'étape 70 et la demande est rejetée.

Si ce n'est pas le cas, alors on passe à l'étape 80.

Dans l'étape 80, l'API vérifie si l'accès à la carte à puce est bloqué par une autre application externe Ae(i) ayant demandé un blocage partiel pour toute application de même classe, c'est-à-dire dont l'octet CLA a pour valeur CLA[Ae(i)]=i :

Si c'est le cas, alors on passe à l'étape 90 où l'API analyse si i=1 :

Si i=1 (les deux applications sont de même classe) alors la demande de connexion de Ae1 est rejetée.

Si i<>1 (les deux applications sont de classes différentes) alors on passe à l'étape 110.

Si ce n'est pas le cas, alors on passe à l'étape 100.

Dans l'étape 100, l'application externe doit demander à l'API si elle désire un blocage total avant de passer à l'étape 130 :

Si ce n'est pas le cas, alors l'accès à la carte à puce sera bloqué pour toute application externe de même classe que l'application Ae(1) donc ayant un octet CLA égal à 1 dans l'étape 110 (réservation partielle de l'API).

Si c'est le cas, alors l'accès à la carte à puce sera bloqué pour toute application externe quelle que soit sa classe dans l'étape 120 (réservation totale de l'API).

Dans l'étape 130, l'application Ae(1) accède à l'application interne correspondante Ai(1) de la carte à puce.

REVENDICATIONS

1. Procédé pour sécuriser l'accès d'une application externe à au moins une carte utilisateur à microprocesseur, ladite carte utilisateur étant susceptible de contenir plusieurs applications internes, ladite application externe correspondant à une des applications internes, ladite carte utilisateur coopérant avec un terminal, ladite application externe utilisant un protocole de connexion à ladite carte utilisateur dans lequel, à chaque type d'application externe est associé un paramètre d'identification prédéterminé, caractérisé en ce que :

- lorsqu'une première application externe est en connexion avec l'application interne correspondante sur ladite carte utilisateur, on détermine le paramètre d'identification de l'application,
- si une deuxième application externe requiert la connexion à ladite carte utilisateur, on analyse le paramètre d'identification de ladite deuxième application,
- si ledit paramètre est identique à celui de la première application connectée, on interdit l'accès pour ladite deuxième application externe à ladite application interne correspondante sur la carte utilisateur.

2. Procédé selon la revendication précédente, dans lequel :
le protocole de connexion entre l'application externe et l'application interne correspondante sur la carte utilisateur résulte d'un échange d'APDU, contenant plusieurs octets, entre l'application externe et l'application interne située sur la carte utilisateur via l'interface logicielle du terminal, ledit paramètre d'identification étant représenté par au moins l'un des octets de l'APDU.

3. Procédé selon la revendication **2**, dans lequel :
au moins l'un des octets de l'APDU est l'octet CLA définissant la classe de l'application externe, chaque type d'application externe identique, susceptible de pouvoir échanger des APDU ayant un octet CLA identique, ledit paramètre d'identification étant l'octet CLA.

4. Procédé selon l'une quelconque des revendications **2 et 3**, caractérisé en ce que l'application externe d'une classe définie ayant effectué une réservation totale de l'accès à au moins une carte utilisateur, l'analyse dudit paramètre d'identification par l'interface logicielle sera effectuée sur toutes les classes possibles qui définissent une application externe.

5. Procédé selon l'une quelconque des revendications précédentes, fonctionnant dans un système de communication permettant une radiocommunication cellulaire, dans lequel lesdits terminaux de communication sont des terminaux de radiocommunication et lesdites cartes utilisateur sont des cartes à puce.

6. Terminal de radiocommunication coopérant avec au moins une carte utilisateur à microprocesseur pour la mise en œuvre du procédé selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il comporte des moyens d'exécution de commandes distincts, des moyens de mémorisation de données distincts pour chaque application de classe distincte et des moyens d'analyse d'au moins un paramètre d'identification contenu dans les données échangées pendant le protocole de connexion.

FIG_1

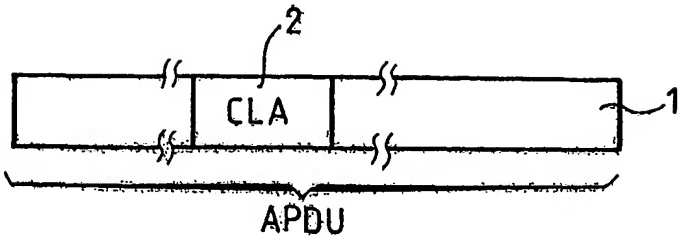

2
CLA
1
APDU

FIG_2

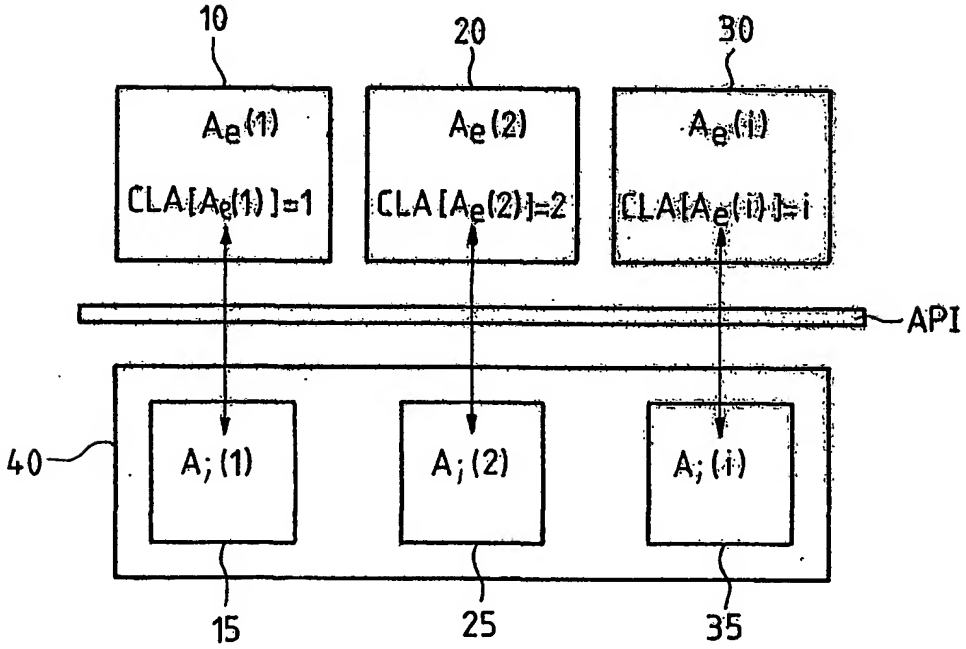
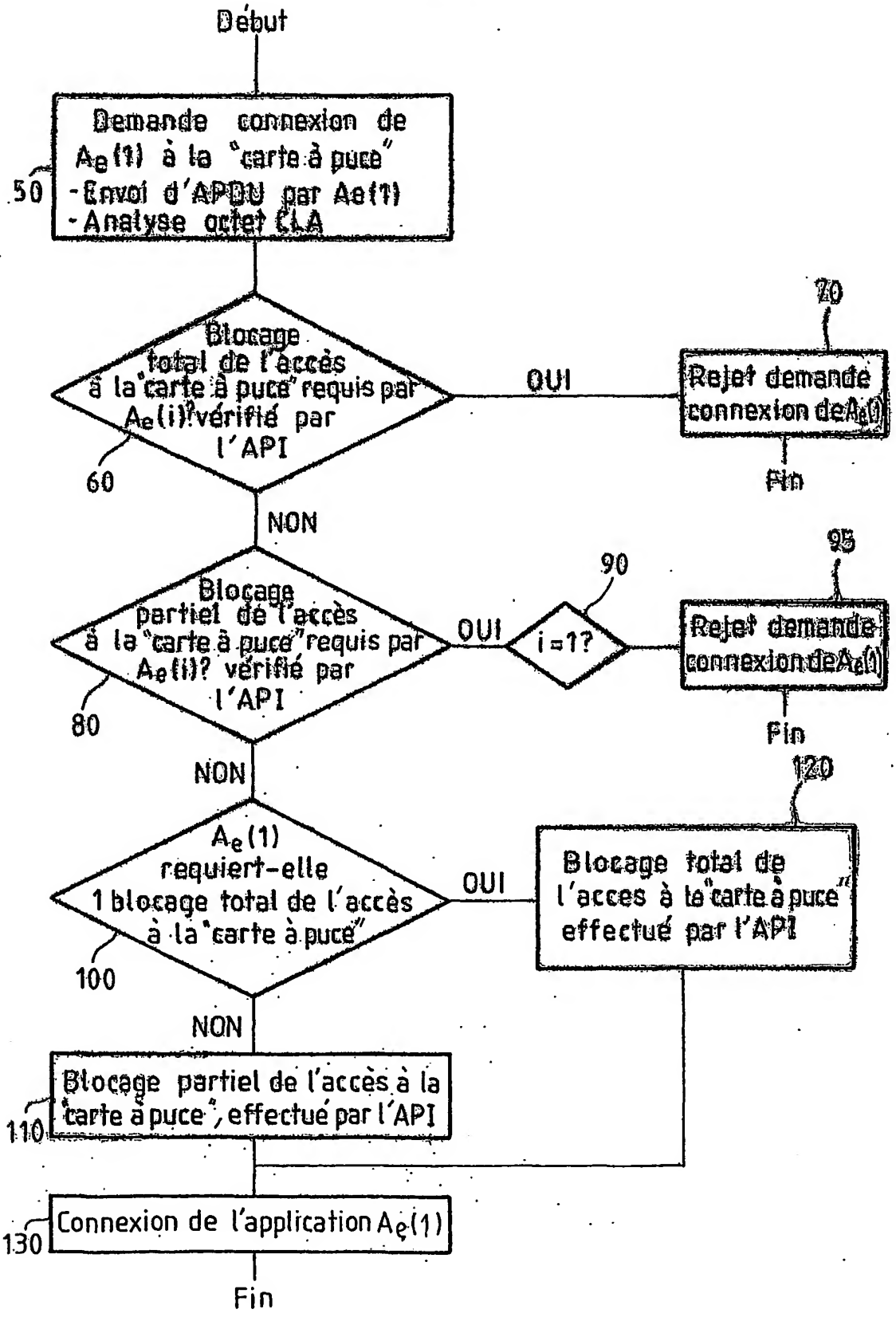

10
20
30
Ae(1)
CLA[Ae(1)]=1
Ae(2)
CLA[Ae(2)]=2
Ae(i)
CLA[Ae(i)]=i
API
40
A;(1)
A;(2)
A;(i)
15
25
35

FIG_3


Début
Demande connexion de Ae(1) à la "carte à puce"
- Envoi d'APDU par Ae(1)
- Analyse octet CLA
50
Blocage total de l'accès à la "carte à puce" requis par Ae(i)? vérifié par l'API
60
OUI
70
Rejet demande connexion de Ae(1)
Fin
NON
Blocage partiel de l'accès à la "carte à puce" requis par Ae(i)? vérifié par l'API
80
OUI
90
i=1?
95
Rejet demande connexion de Ae(1)
Fin
NON
Ae(1) requiert-elle 1 blocage total de l'accès à la "carte à puce"
100
OUI
120
Blocage total de l'acces à la "carte à puce" effectué par l'API
NON
Blocage partiel de l'accès à la "carte à puce", effectué par l'API
110
Connexion de l'application Ae(1)
130
Fin

INTERNATIONAL SEARCH REPORT

In nal Application No
PCT/FR 01/02489

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F9/46 G07F7/10 H04Q7/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07F H04Q G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 6 092 133 A (EROLA MIKA ET AL) 18 July 2000 (2000-07-18) column 1, line 30 - line 33 column 2, line 62 - line 66 column 4, line 1 - line 9 column 4, line 35 - line 38 column 8, line 31 -column 9, line 7 column 11, line 24 - line 27 figures 4-8	1-6
A	WO 98 52159 A (MONDEX INT LTD) 19 November 1998 (1998-11-19) page 3, line 13 -page 14, line 10	

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
9 October 2001	16/10/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016	Kampouris, A

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inte I Application No
PCT/FR 01/02489

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6092133 A	18-07-2000	FI 965071 A	18-06-1998
		AU 733031 B2	03-05-2001
		AU 5399098 A	15-07-1998
		CN 1245620 A	23-02-2000
		EP 0976273 A1	02-02-2000
		WO 9827767 A1	25-06-1998
		JP 2001508253 T	19-06-2001
WO 9852159 A	19-11-1998	US 6220510 B1	24-04-2001
		AU 736325 B2	26-07-2001
		AU 6299698 A	09-09-1998
		AU 7776798 A	08-12-1998
		AU 7776898 A	08-12-1998
		AU 7776998 A	08-12-1998
		AU 7777098 A	08-12-1998
		AU 7777198 A	08-12-1998
		AU 7777298 A	08-12-1998
		AU 7777398 A	08-12-1998
		AU 7777498 A	08-12-1998
		EP 0963580 A1	15-12-1999
		EP 0981807 A2	01-03-2000
		EP 0985202 A1	15-03-2000
		EP 0985203 A1	15-03-2000
		EP 0976114 A2	02-02-2000
		EP 0985204 A1	15-03-2000
		EP 0981805 A1	01-03-2000
		WO 9837526 A1	27-08-1998
		WO 9852158 A2	19-11-1998
		WO 9852159 A2	19-11-1998
		WO 9852160 A2	19-11-1998
		WO 9852161 A2	19-11-1998
		WO 9852152 A2	19-11-1998
		WO 9852162 A2	19-11-1998
		WO 9852163 A2	19-11-1998
		WO 9852153 A2	19-11-1998
		US 6230267 B1	08-05-2001
		US 6164549 A	26-12-2000

RAPPORT DE RECHERCHE INTERNATIONALE

De Internationale No
PCT/FR 01/02489

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G06F9/46 G07F7/10 H04Q7/32

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 G07F H04Q G06F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	US 6 092 133 A (EROLA MIKA ET AL) 18 juillet 2000 (2000-07-18) colonne 1, ligne 30 - ligne 33 colonne 2, ligne 62 - ligne 66 colonne 4, ligne 1 - ligne 9 colonne 4, ligne 35 - ligne 38 colonne 8, ligne 31 -colonne 9, ligne 7 colonne 11, ligne 24 - ligne 27 figures 4-8	1-6
A	WO 98 52159 A (MONDEX INT LTD) 19 novembre 1998 (1998-11-19) page 3, ligne 13 -page 14, ligne 10	

☐ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
9 octobre 2001	16/10/2001

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Kampouris, A

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Der nternationale No
PCT/FR 01/02489

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
US 6092133	A	18-07-2000	FI	965071 A	18-06-1998
			AU	733031 B2	03-05-2001
			AU	5399098 A	15-07-1998
			CN	1245620 A	23-02-2000
			EP	0976273 A1	02-02-2000
			WO	9827767 A1	25-06-1998
			JP	2001508253 T	19-06-2001
WO 9852159	A	19-11-1998	US	6220510 B1	24-04-2001
			AU	736325 B2	26-07-2001
			AU	6299698 A	09-09-1998
			AU	7776798 A	08-12-1998
			AU	7776898 A	08-12-1998
			AU	7776998 A	08-12-1998
			AU	7777098 A	08-12-1998
			AU	7777198 A	08-12-1998
			AU	7777298 A	08-12-1998
			AU	7777398 A	08-12-1998
			AU	7777498 A	08-12-1998
			EP	0963580 A1	15-12-1999
			EP	0981807 A2	01-03-2000
			EP	0985202 A1	15-03-2000
			EP	0985203 A1	15-03-2000
			EP	0976114 A2	02-02-2000
			EP	0985204 A1	15-03-2000
			EP	0981805 A1	01-03-2000
			WO	9837526 A1	27-08-1998
			WO	9852158 A2	19-11-1998
			WO	9852159 A2	19-11-1998
			WO	9852160 A2	19-11-1998
			WO	9852161 A2	19-11-1998
			WO	9852152 A2	19-11-1998
			WO	9852162 A2	19-11-1998
			WO	9852163 A2	19-11-1998
			WO	9852153 A2	19-11-1998
			US	6230267 B1	08-05-2001
			US	6164549 A	26-12-2000